PLAN DU SOUS SAVOIR S32

A. Présentation du routage et du transfert de paquets.

I. Présentation du routage

Le routage est le processus qu'un routeur utilise pour transmettre des paquets vers un réseau de destination. Un routeur prend des décisions en fonction de l'adresse IP de destination d'un paquet. Tout le long du chemin, les divers équipements se servent de l'adresse IP de destination pour orienter le paquet dans la bonne direction afin qu'il arrive à destination.

II. Principe du routage des paquets IP

Lors de l'émission, le protocole découpe les données en petits paquets (souvent appelés datagrammes IP). Ces paquets ont tous la même structure :

EN-TETE	ZONE DE DONNEES

Datagramme IP

C'est l'en-tête qui contient, entre autre, les adresses de l'émetteur et du destinataire. Un appareil chargé du routage analysera l'adresse du destinataire afin d'aiguiller le paquet vers le prochain routeur menant à sa destination.

2.1. Chaque appareil possède une table de routage gérée par le logiciel IP

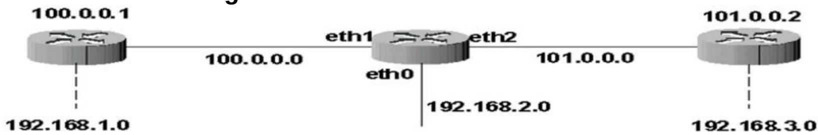
Une table de routage est une liste contenant essentiellement trois types d'informations : des adresses réseau avec le masque réseau associé et le moyen de les atteindre. Soit le réseau est directement connecté à l'appareil, dans ce cas le moyen de l'atteindre est le nom de l'interface, soit, il s'agit de l'adresse du prochain routeur situé sur la route vers ce réseau. Par exemple, considérons sur un appareil quelconque, sa table de routage :

Tableau 1. Table de routage

Réseau	Masque	Moyen de l'atteindre
192.168.2.0	255.255.255.0	eth0
100.0.0.0	255.0.0.0	eth1
101.0.0.0	255.0.0.0	eth2
192.168.1.0	255.255.255.0	100.0.0.1
192.168.3.0	255.255.255.0	101.0.0.2

Cette table est riche d'informations. On apprend très précisément que l'appareil possède trois interfaces réseau (eth0, eth1, eth2) ainsi que les adresses IP des réseaux qui sont directement reliés à ces interfaces. On connaît les adresses IP de deux routeurs. On sait qu'il existe deux réseaux 192.168.1.0 et 192.168.3.0 et qu'ils sont respectivement derrière les routeurs 100.0.0.1 et 101.0.0.2. En revanche, il est impossible d'affirmer que ces deux réseaux sont directement reliés à ces routeurs. Pour résumer, on peut dresser le schéma suivant :

Topologie d'après une table de routage



Quelques observations complémentaires :

- Étant donné que l'appareil observé possède trois interfaces, c'est très probablement un routeur. Cependant, notez que tout appareil fonctionnant sous TCP/IP possède une table de routage (qu'il soit routeur ou non).
- Pour que le routage fonctionne, il est impératif que toutes les interfaces réseau possédant le même préfixe réseau soient reliées au même réseau physique.

2.2. Tous les appareils sous IP exécutent le même algorithme

Lors de l'émission d'un paquet de données, le logiciel IP recherche une correspondance dans la table en appliquant le masque réseau de chaque ligne avec l'adresse IP de destination du paquet. Notez qu'il parcourt la table dans l'ordre décroissant des masques afin de garantir la correspondance la plus précise entre l'adresse dans la table et l'adresse de destination (*best match*).

Au total, seules quatre possibilités sont imaginables :

- Ce préfixe correspond à celui d'un réseau directement connecté ; il y a remise directe du paquet sur le réseau et le routage est terminé.
- Ce préfixe correspond à celui d'un réseau accessible via un routeur on récupère l'adresse physique de ce routeur et on lui transmet le paquet. Notez que l'adresse IP de l'émetteur reste inchangée.
- Ce préfixe n'a pas de correspondance dans la table mais il existe un routeur par défaut dans la table ; on transmet au routeur par défaut.
- Si aucun des trois cas précédents n'est rempli, on déclare une erreur de routage.

2.3. Exemple de table de routage IP de Windows

Chaque ordinateur exécutant TCP/IP prend des décisions de routage. Celles-ci sont contrôlées par la table de routage IP. Pour afficher la table de routage IP sur un ordinateur exécutant Windows XP, vous pouvez taper « route print » à l'invite de commandes.
Le tableau suivant illustre un exemple de table de routage IP. Cet exemple s'applique à un ordinateur exécutant Windows XP avec une carte réseau et la configuration suivante :

Adresse IP : 10.0.0.169
Masque de sous-réseau : 255.0.0.0
Passerelle par défaut : 10.0.0.1

Description	Réseau de destination	Masque de réseau	Passerelle	Interface	Métrique
Itinéraire par défaut	0.0.0.0	0.0.0.0	10.0.0.1	10.0.0.169	1
Réseau de bouclage	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
Réseau local	10.0.0.0	255.0.0.0	10.0.0.169	10.0.0.169	1
Adresse IP locale	10.0.0.169	255.255.255.255	127.0.0.1	127.0.0.1	1
Adresses multidestinataires	224.0.0.0	240.0.0.0	10.0.0.169	10.0.0.169	1
Adresse de diffusion limitée	255.255.255.255	255.255.255.255	10.0.0.169	10.0.0.169	1

Notes

- Les descriptions de la première colonne du tableau précédent ne sont pas actuellement affichées à la sortie de la commande route print.
- La table de routage est automatiquement créée, en fonction de la configuration TCP/IP actuelle de votre ordinateur. Chaque itinéraire occupe une seule ligne dans le tableau affiché. Votre ordinateur recherche dans la table de routage une entrée qui correspondrait le mieux à l'adresse de destination IP en commençant par le masque le plus grand.
- Votre ordinateur utilise l'itinéraire par défaut si aucun autre itinéraire d'hôte ou de réseau ne correspond à l'adresse de destination intégrée dans un datagramme IP. L'itinéraire par défaut transmet généralement un datagramme IP (pour lequel il n'existe pas d'itinéraire local correspondant ou explicite) dans une adresse de passerelle par défaut pour un routeur du sous-réseau local. Dans l'exemple précédent, l'itinéraire par défaut transmet le datagramme vers un routeur avec une adresse de passerelle 10.0.0.1.
- Étant donné que le routeur qui correspond à la passerelle par défaut contient des informations relatives au réseau dans l'Internet, il transmet le datagramme vers les autres routeurs jusqu'à ce que le datagramme soit éventuellement livré à un routeur IP connecté à l'hôte ou au sous-réseau de destination spécifié dans le réseau le plus grand.

Les sections suivantes décrivent chacune des colonnes affichées dans la table de routage IP : destination du réseau, masque de réseau, passerelle, interface et métrique.

- **Destination du réseau**
  La destination du réseau est utilisée avec le masque de réseau pour correspondre à l'adresse de destination IP du paquet. Cette destination est comprise entre 0.0.0.0 pour l'itinéraire par défaut et 255.255.255.255 pour la diffusion limitée qui est une adresse de diffusion spéciale vers tous les hôtes du même segment de réseau.
- **Masque de réseau**
  Le masque de réseau est le masque de sous-réseau appliqué à l'adresse de destination IP lors d'une comparaison à la valeur du réseau de destination du paquet. Lorsque le masque de réseau est au format binaire, les " 1 " doivent concorder, mais pas les " 0 ". Par exemple, un masque de réseau 0.0.0.0 est utilisé pour l'itinéraire par défaut, ce qui signifie qu'aucun des bits ne doit concorder. Pour les itinéraires d'hôtes on utilise une adresse IP avec un masque réseau 255.255.255.255.
- **Passerelle**
  L'adresse de la passerelle est l'adresse IP que l'hôte local utilise pour transmettre les datagrammes IP vers d'autres réseaux IP. Il s'agit soit de l'adresse IP d'une carte réseau locale, soit de l'adresse IP d'un routeur IP (tel que le routeur de la passerelle par défaut) sur le segment de réseau local.

- **Interface**
  L'interface est l'adresse IP configurée sur l'ordinateur local pour la carte réseau local utilisée lorsqu'un datagramme IP est transmis sur le réseau.
- **Métrique**
  Une métrique indique le coût de l'utilisation d'un itinéraire qui correspond généralement au nombre de relais vers la destination IP. Un saut correspond à tout ce qui se trouve sur le sous-réseau local. Chaque routeur utilisé au-delà de ce premier saut correspond à un saut supplémentaire. S'il existe plusieurs itinéraires vers la même destination avec différentes métriques, l'itinéraire présentant la métrique la plus faible est sélectionnée.

2.4. Commande « route »

Gère les tables de routage du réseau. Cette commande est disponible uniquement si le protocole TCP/IP est installé.

route [-f] [-p] [*commande* [*destination*] [masque *masque_sous-réseau*] [*passerelle*] [métrique *coût_métrique*]]

Paramètres :

-f Efface les tables de routage de toutes les entrées.

-p Associé à la commande add, ce paramètre crée une route persistante au travers des amorçages du système. Par défaut, les routes ne sont pas maintenues lorsque le système est relancé. Associé à la commande print, ce paramètre affiche la liste des routes persistantes enregistrées. Ce paramètre est ignoré pour toutes les autres commandes qui affectent systématiquement les routes persistantes appropriées.

- ***commande :*** spécifie une des commandes suivantes :

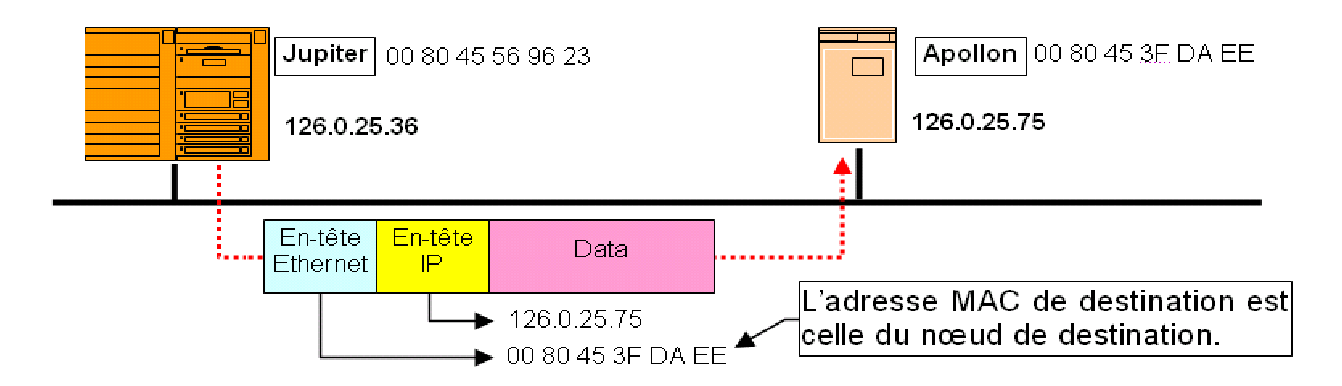
print	Imprime une route.
add	Ajoute une route.
delete	Supprime une route.
change	Modifie une route existante.

- ***destination :*** spécifie le réseau auquel est destiné le paquet.
- **masque *masque_sous-réseau* :** spécifie le masque de sous-réseau à associer à cette entrée d'itinéraire. Si le masque n'est pas spécifié, 255.255.255.255 est utilisé.
- ***passerelle :*** spécifie la passerelle vers laquelle sont envoyés les paquets pour atteindre le réseau de destination.
- **métrique *coût_métrique* :** assigne un coût métrique entier (entre 1 et 9 999) à utiliser pour calculer les routes les plus rapides, fiables et/ou économiques.

III. Routage direct et indirect

- **Routage direct**

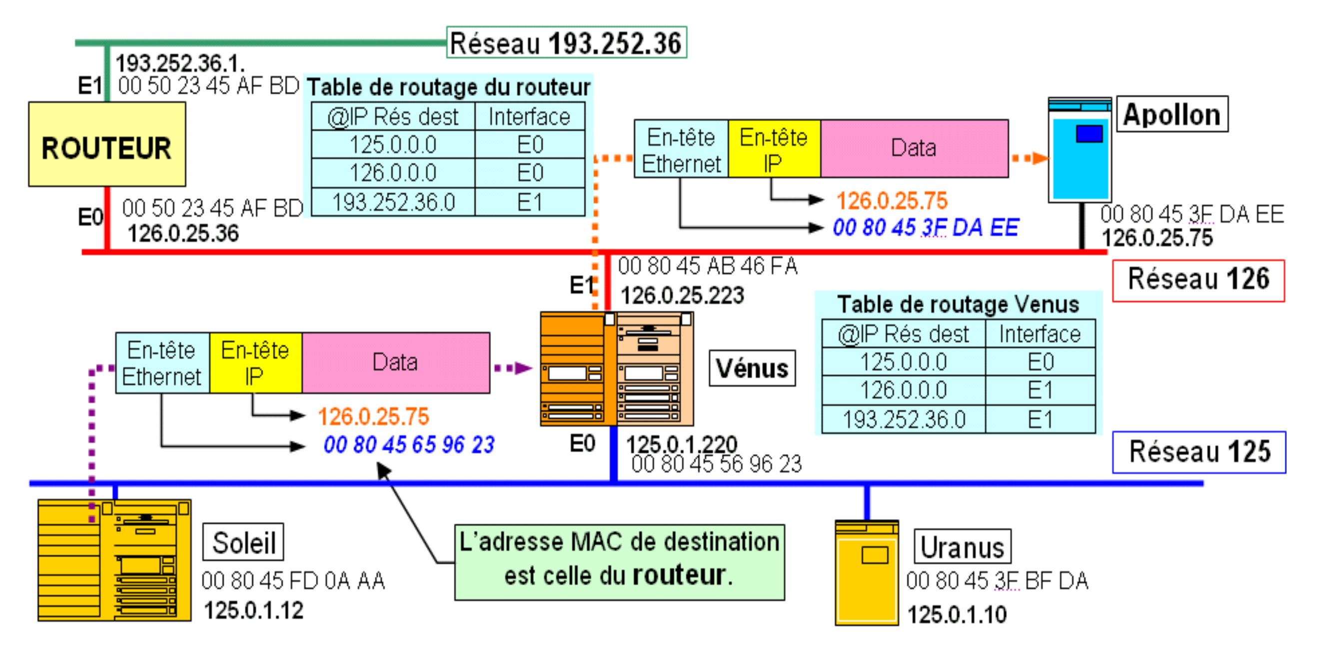
Le routage direct est la transmission d'un datagramme d'une station à une autre à l'intérieur d'un même réseau. Lorsque la couche **IP** reçoit les données à transmettre, elle cherche dans la table de routage si la station de destination est sur le même réseau ou si le datagramme doit transiter par un routeur. Dans l'exemple suivant, la machine destination étant sur le même réseau, le datagramme est passé à la couche liaison qui utilise ARP pour trouver l'adresse physique de destination et l'incorpore dans l'en-tête Ethernet.



- **Routage indirect**

Le routage indirect fait apparaître la notion de **routeur**. Quand un datagramme IP est envoyé d'un réseau vers un autre réseau (voir l'exemple suivant), les parties "réseau" des adresses IP source (125) et destination (126) sont différentes. Dans ce cas, la station émettrice envoie le paquet au routeur qui relie les 2 réseaux en utilisant l'adresse physique de ce dernier. Le routeur utilise l'adresse IP pour reconnaître le réseau et la station auxquels il doit envoyer ce paquet. Chaque routeur possède pour chacun des réseaux sur lequel il est connecté, une cache ARP entre les adresses IP et les adresses Physiques.

Le routeur dans l'exemple suivant est l'ordinateur **Vénus**. Il comporte 2 cartes réseau, donc 2 adresses MAC et 2 adresses IP correspondant à des numéros de réseaux différents.
Si la machine **Soleil** veut envoyer un datagramme IP vers la machine **Apollon**, la couche IP recherche l'adresse IP de destination dans la table de routage et détermine le routeur auquel il faut transmettre le paquet.



Le processus suivant est utilisé :

- recherche de l'adresse **IP destination complète**, si elle existe dans la table, pour déterminer l'adresse du prochain routeur sur le chemin emprunté pour atteindre la destination.
- si l'adresse complète n'est pas trouvée, la couche IP essaye d'utiliser **l'adresse réseau** destination (126) et le routeur correspondant.
- si l'adresse réseau destination n'est pas non plus trouvée dans la table, IP utilise l'adresse du **routeur par défaut** (125.0.1.220).

En utilisant le contenu du cache ARP présent dans **Soleil**, la couche IP insère le datagramme dans une trame Ethernet avec comme adresse destination MAC celle du routeur **Vénus** connectée au réseau 125 (00 80 45 56 96 23). L'adresse de destination IP est celle d'**Apollon**. Dans le routeur, IP analyse l'adresse de destination IP. Après consultation de la table de routage et du cache ARP, une trame Ethernet avec l'adresse MAC d'Apollon (00 80 45 3F DA EE) est envoyée sur le réseau 126 avec comme adresse de destination IP 126.0.25.75.

IV. Routage statique et dynamique.

Pour prendre les bonnes décisions, les routeurs doivent connaître la direction à prendre jusqu'aux réseaux distants. Lorsque les routeurs utilisent le routage dynamique, ces informations sont fournies par les autres routeurs. Lorsque le routage statique est utilisé, un administrateur réseau configure manuellement les informations sur les réseaux distants.

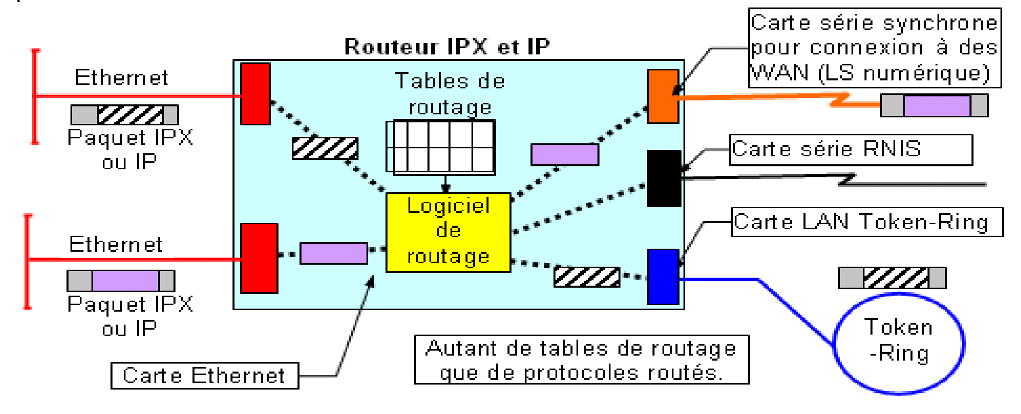
B. Configuration de base des routeurs CISCO.

I . Vue d'ensemble de l'architecture des routeurs Cisco.

a. Structure d'un routeur.

Les routeurs peuvent être :

- des boîtiers dédiés possédant plusieurs interfaces correspondant à des types de réseaux différents ou identiques. Par exemple les routeurs CISCO ou Nortel. Chaque routeur possède son propre système d'exploitation. Le système d'exploitation des routeurs CISCO est appelé IOS.
- la fonction routage peut aussi être implémentée dans les serveurs travaillant avec des systèmes d'exploitation comme Unix, Windows ou NetWare.

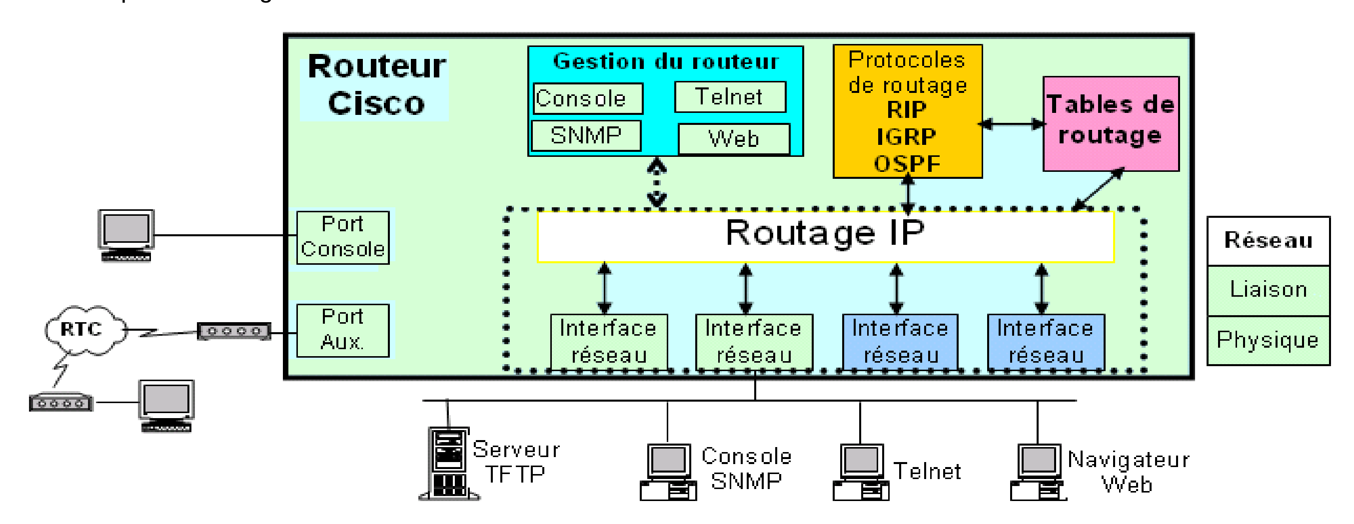


b. Configuration d'un routeur.

Les routeurs doivent être configurés manuellement ou en chargeant un fichier de configuration. Il faut au minimum entrer les adresses IP et les masques de sous-réseaux des interfaces du routeur.

La configuration des routeurs se fera :

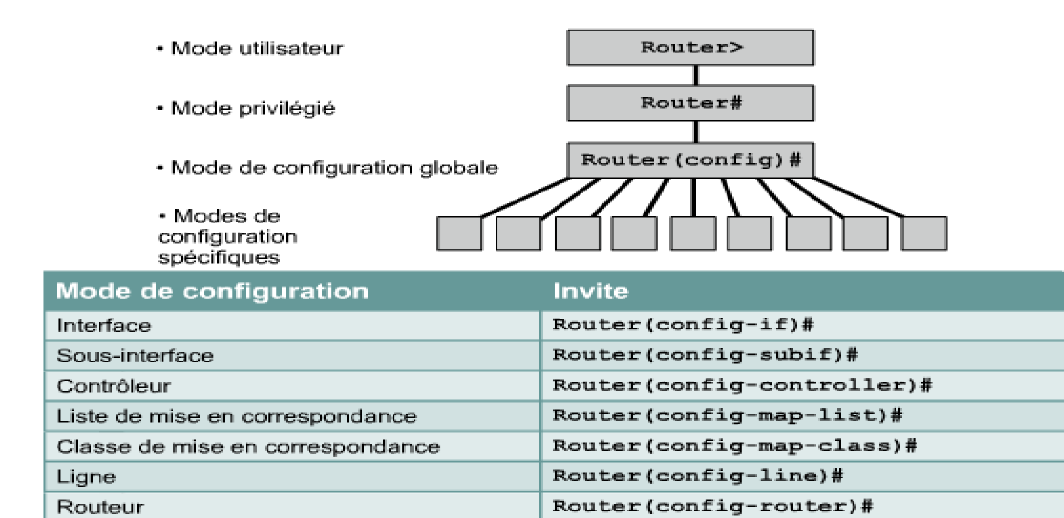
- par un terminal connecté sur le port console.
- par Telnet en utilisant le réseau.
- par un logiciel propriétaire en réseau s'appuyant sur SNMP.
- dans certains cas, un petit serveur Web est implémenté dans le routeur et on utilise un navigateur pour la configuration.



II. Configuration de base d'un routeur CISCO

a. Modes de commande CLI

Toutes les modifications de la configuration de l'interface de commande en ligne (CLI) apportées sur un routeur Cisco sont effectuées en mode de configuration globale. D'autres modes spécifiques sont activés en fonction de la modification de configuration requise, mais ces modes sont tous des sous-ensembles du mode de configuration globale.



Mode de configuration	Invite
Interface	Router(config-if)#
Sous-interface	Router(config-subif)#
Contrôleur	Router(config-controller)#
Liste de mise en correspondance	Router(config-map-list)#
Classe de mise en correspondance	Router(config-map-class)#
Ligne	Router(config-line)#
Routeur	Router(config-router)#
Routeur IPX	Router(config-ipx-router)#
Mise en correspondance de route	Router(config-route-map)#

Les commandes de configuration globale sont utilisées sur un routeur pour appliquer des instructions de configuration qui affectent l'ensemble du système. La commande suivante place le routeur en mode de configuration globale et permet d'entrer des commandes à partir du terminal :

Router#**configure terminal**
Router(config)#

Le mode de configuration globale (global config) est le mode de configuration principal. Voici quelques-uns des modes auquel vous pouvez accéder à partir du mode de configuration globale :

- Mode interface
- Mode ligne
- Mode routeur
- Mode sous-interface
- Mode contrôleur

Lorsque vous passez dans ces modes spécifiques, l'invite du routeur se transforme pour indiquer le mode de configuration particulier. Toute modification de la configuration effectuée s'applique uniquement aux interfaces ou aux processus couverts par le mode particulier.

Si vous tapez exit alors que vous êtes dans l'un de ces modes de configuration spécifiques, le routeur retourne en mode de configuration globale. Si vous appuyez sur les touches Ctrl-Z, vous quittez les modes de configuration et vous revenez au mode privilégié

b. Configuration du nom d'un routeur

L'une des premières tâches de configuration consiste à attribuer au routeur un nom unique. Pour ce faire, vous devez, en mode de configuration globale, utiliser les commandes suivantes:

Router(config)#**hostname Tokyo**
Tokyo(config)#

Dès que vous appuyez sur la touche **Entrée**, l'invite passe du nom d'hôte par défaut (Router) au nom d'hôte nouvellement configuré, c'est-à-dire Tokyo, dans notre exemple.

c. Configuration des mots de passe d'un routeur

Les mots de passe limitent l'accès aux routeurs. Ils doivent toujours être configurés pour les lignes de terminal virtuel et pour la ligne de console. Les mots de passe sont également utilisés pour contrôler l'accès au mode

privilégié pour que seuls les utilisateurs autorisés puissent apporter des modifications au fichier de configuration.

Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne de console :

Router(config)#**line console 0**
Router(config-line)#**password** <*password*>
Router(config-line)#**login**

Pour que les utilisateurs puissent accéder à distance au routeur à l'aide de Telnet, un mot de passe doit être défini sur une ou plusieurs lignes de terminal virtuel (VTY). En règle générale, les routeurs Cisco prennent en charge cinq lignes VTY numérotées de 0 à 4, bien que chaque plate-forme matérielle prenne en charge des numéros différents sur les connexions VTY. Le même mot de passe est souvent utilisé pour toutes les lignes, mais il arrive parfois qu'une ligne soit définie pour fournir au routeur une entrée de secours si les quatre autres connexions sont utilisées. Les commandes suivantes sont utilisées pour définir le mot de passe sur les lignes VTY:

Router(config)#**line vty 0 4**
Router(config-line)#**password** <*password*>
Router(config-line)#**login**

Le mot de passe enable et le mot de passe enable secret sont utilisés pour limiter l'accès au mode privilégié. Seul le mot de passe enable est utilisé si le mot de passe enable secret n'a pas été défini. Il est recommandé de définir et d'utiliser uniquement le mot de passe enable secret car, contrairement au mot de passe enable, il est crypté. Les commandes suivantes permettent de définir les mots de passe enable :

Router(config)#**enable password** <*password*>
Router(config)#**enable secret** <*password*>

Il est parfois préférable que les mots de passe ne soient pas affichés en texte clair dans le résultat des commandes show running-config ou show startup-config. Cette commande permet de crypter les mots de passe dans le résultat de configuration:

Router(config)#**service password-encryption**
La commande **service password-encryption** applique un cryptage simple à tous les mots de passe non cryptés. La commande **enable secret**<*password*> utilise un puissant algorithme MD5 pour le cryptage.

d. Examen des commandes show

Plusieurs commandes show peuvent être utilisées pour examiner le contenu des fichiers du routeur ou pour le dépannage. Dans le mode privilégié et le mode utilisateur, la commande show ? présente une liste des commandes show disponibles. Cette liste est beaucoup plus longue en mode privilégié qu'en mode utilisateur.

- **show interfaces**: Affiche les statistiques relatives à toutes les interfaces du routeur. Pour afficher les statistiques d'une interface spécifique, entrez la commande **show interfaces**, suivie par le numéro spécifique de l'interface et du port. Exemple:

  Router#**show interfaces serial 0/1**
- **show controllers serial**:Affiche les caractéristiques de l'interface. Cette commande doit indiquer le port ou l'emplacement et le numéro de port (slot/port number) de l'interface série. Par exemple:

  Router#**show controllers serial 0/1**
- **show clock**: Indique l'heure définie sur le routeur
- **show hosts**: Affiche une liste de noms et d'adresses d'hôtes se trouvant en mémoire cache
- **show users**: Indique tous les utilisateurs connectés au routeur
- **show history**: Affiche un historique des commandes qui ont été saisies
- **show flash**: Affiche des informations sur la mémoire flash ainsi que la liste des fichiers IOS qui y sont stockés
- **show version**: Affiche des informations sur le logiciel actuellement chargé en mémoire ainsi que sur les caractéristiques du matériel et de l'équipement.

- **show ARP**: Affiche la table ARP du routeur
- **show protocols**: Affiche l'état général et propre aux interfaces de tous les protocoles de couche 3 configurés.
- **show startup-config**: Affiche le contenu de la NVRAM si elle est disponible et valide ou montre le fichier de configuration référencé par la variable d'environnement CONFIG_FILE.
- **show running-config**: Affiche le contenu du fichier de configuration exécuté actuellement en mémoire.

e. Configuration d'une interface série

Une interface série peut être configurée depuis la console ou par l'intermédiaire d'une ligne de terminal virtuel. Pour configurer une interface série, procédez comme suit:

1. Passez en mode de configuration globale
2. Passez en mode interface
3. Spécifiez l'adresse et le masque de sous-réseau de l'interface
4. Si un câble ETCD est connecté, définissez la fréquence d'horloge. Ignorez cette étape si c'est un câble ETTD qui est connecté.
5. Activez l'interface

Si l'interface est destinée à acheminer des paquets IP, chaque interface série connectée doit posséder une adresse IP et un masque de sous-réseau. Configurez l'adresse IP à l'aide des commandes suivantes :

Router(config)#**interface serial 0/0**
Router(config-if)#**ip address** *<ip address> <net mask>*

Les interfaces série nécessitent un signal d'horloge pour contrôler la synchronisation des communications. Dans la plupart des environnements, un équipement ETCD fournira cette synchronisation. Par défaut, les routeurs Cisco sont des équipements ETTD, mais ils peuvent être configurés en tant qu'équipements ETCD.

Sur les liaisons série qui sont directement interconnectées, comme dans un environnement de TP, un des côtés doit être considéré comme un équipement ETCD et fournir le signal de synchronisation. L'horloge est activée et sa fréquence est spécifiée à l'aide de la commande clock rate. Les fréquences d'horloge (en bits par seconde) sont les suivantes : 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 ou 4000000. Cependant, certains de ces paramètres peuvent ne pas être disponibles sur certaines interfaces série, en raison de leur capacité.

Par défaut, les interfaces sont mises hors tension ou désactivées. Pour mettre sous tension ou activer une interface, la commande no shutdown est exécutée. S'il est nécessaire de désactiver une interface en vue d'une opération de maintenance ou de dépannage, la commande shutdown est utilisée pour mettre l'interface hors tension.

Dans l'environnement de TP, nous utiliserons la valeur 56000 comme fréquence d'horloge. Les commandes qui permettent de définir une fréquence d'horloge et d'activer une interface série sont les suivantes:

Router(config)#**interface serial 0/0**
Router(config-if)#**clock rate 56000**
Router(config-if)#**no shutdown**

f. Configuration d'une interface Ethernet

Une interface Ethernet peut être configurée depuis la console ou par l'intermédiaire d'une ligne de terminal virtuel.

```
Router(config)#interface e0
Router(config-if)#ip address 183.8.126.2 255.255.255.128
Router(config-if)#no shutdown
```

Si l'interface est destinée à acheminer des paquets IP, chaque interface Ethernet doit posséder une adresse IP et un masque de sous-réseau.

Pour configurer une interface Ethernet, procédez comme suit:

1. Passez en mode de configuration globale
2. Passez en mode de configuration d'interface
3. Spécifiez l'adresse et le masque de sous-réseau de l'interface
4. Activez l'interface

Par défaut, les interfaces sont mises hors tension ou désactivées. Pour mettre sous tension ou activer une interface, la commande no shutdown est exécutée. S'il est nécessaire de désactiver une interface en vue d'une opération de maintenance ou de dépannage, la commande shutdown est utilisée pour mettre l'interface hors tension.

g. Faire des changements de configuration

Si une configuration doit être modifiée, passez dans le mode approprié et exécutez la commande nécessaire. Par exemple, pour activer une interface, passez en mode de configuration globale, en mode interface, puis lancez la commande **no shutdown**.

Pour vérifier les modifications, utilisez la commande show running-config. Cette commande affiche la configuration courante. Si les variables affichées ne correspondent pas à celles prévues, vous pouvez corriger l'environnement en effectuant une ou plusieurs des opérations suivantes:

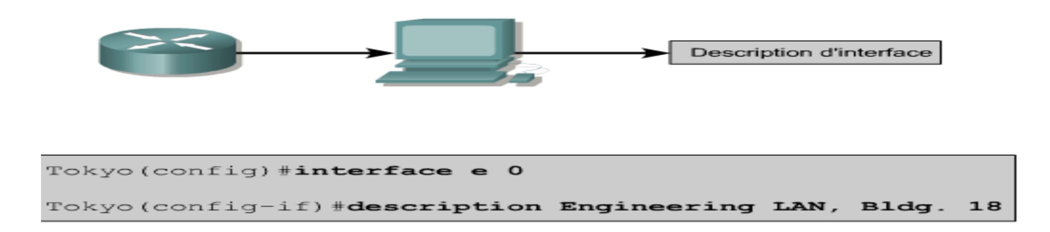
- entrer la forme négative (**no**) d'une commande de configuration,
- recharger le système afin de rétablir le fichier de configuration d'origine de la mémoire NVRAM,
- copier un fichier de configuration archivé à partir d'un serveur TFTP,
- supprimer le fichier de configuration de démarrage à l'aide de **erase startup-config**, puis le redémarrer et passer en mode setup.

Pour enregistrer les variables de configuration dans le fichier de configuration de démarrage de la mémoire NVRAM, entrez la commande suivante à l'invite du mode privilégié:

Router#**copy running-config startup-config**

h. Descriptions d'interface

Il est indispensable d'utiliser une description d'interface afin d'identifier des informations importantes concernant par exemple un routeur, un numéro de circuit ou un segment de réseau spécifique. En se reportant à cette description, un utilisateur de réseau pourra se souvenir d'informations spécifiques sur l'interface, telle que le réseau qu'elle dessert.



La description se limite à un commentaire à propos de l'interface. Bien qu'elle figure dans les fichiers de configuration qui sont stockés dans la mémoire du routeur, la description n'affecte en rien son fonctionnement. Les descriptions sont créées en respectant un format standard qui s'applique à chaque interface. La description peut inclure l'emplacement et le rôle de l'interface, les autres unités ou emplacements connectés à l'interface et les identificateurs de circuit. Grâce aux descriptions, les personnels de support comprennent mieux l'incidence des problèmes liés à une interface et peuvent résoudre les problèmes plus rapidement.

i. Configuration d'une description d'interface

Pour configurer une description d'interface, passez en mode configuration globale. À partir de ce mode, passez en mode de configuration d'interface. Utilisez la commande **description**, suivie des informations.

Étapes de la procédure:

Passez en mode de configuration globale en entrant la commande **configure terminal**.

Passez en mode d'interface spécifique (par exemple interface Ethernet 0) **interface ethernet 0**.

Entrez la description de la commande, suivie des informations que vous voulez voir s'afficher. Par exemple, Réseau XYZ, Immeuble 18.

Revenez en mode privilégié à l'aide de la commande **ctrl-Z**.

Enregistrez en mémoire NVRAM les modifications de la configuration à l'aide de la commande **copy running-config startup-config**.

Voici deux exemples de descriptions d'interface:

interface Ethernet 0
description LAN Engineering, Bldg.2
interface serial 0
description ABC network 1, Circuit 1

j. Bannières de connexion

Comme son nom l'indique, une bannière de connexion s'affiche lors de la connexion, et permet de transmettre un message destiné à tous les utilisateurs du routeur (pour les avertir, par exemple, d'un arrêt imminent du système).

Ces bannières de connexion peuvent être lues par tout le monde. Par conséquent, vous devez faire très attention à la formule choisie pour le message de la bannière. Un message "Bienvenue" qui invite tout le monde à entrer n'est probablement pas approprié.

```
LAB_A con0 is now available

Press RETURN to get started.

This is a secure system.  Authorized Access ONLY!!!

User Access Verification

Password:

LAB_A>enable

Password:

LAB_A#
```

On préfèrera par exemple un avertissement indiquant de ne pas tenter de se connecter sans autorisation. Par exemple, un message tel que "Système sécurisé. Accès autorisé uniquement !" indique aux visiteurs indésirables que toute intrusion est interdite et illégale.

k. Résolution de nom d'hôte

La résolution de nom d'hôte est le processus qu'utilise le système informatique pour associer un nom d'hôte à une adresse IP.

Pour pouvoir utiliser des noms d'hôtes afin de communiquer avec d'autres unités IP, les équipements réseau tels que les routeurs doivent être en mesure d'associer les noms d'hôte aux adresses IP. Une liste de noms d'hôtes et de leurs adresses IP associées a pour nom table d'hôtes.

Voici un exemple de configuration de table d'hôtes sur un routeur :

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Une table d'hôtes peut inclure tous les équipements d'une organisation de réseau. Un nom d'hôte peut être associé à chaque adresse IP unique. La plate-forme logicielle Cisco IOS conserve en mémoire cache les correspondances nom d'hôte-adresse de sorte que les commandes d'exécution puissent les utiliser. Cette mémoire cache accélère le processus de conversion des noms en adresses.

Contrairement aux noms DNS, les noms d'hôtes ne sont significatifs que sur le routeur sur lequel ils sont configurés. La table d'hôtes permettra à l'administrateur réseau de taper soit le nom d'hôte proprement dit, comme Auckland, soit l'adresse IP pour l'envoi d'une requête Telnet à un hôte distant.

l. Configuration des tables d'hôtes

Pour attribuer des tables d'hôtes aux adresses, passez d'abord en mode de configuration globale. Entrez la commande **ip host**, suivie du nom de la destination et de toutes les adresses IP où l'équipement est accessible. Cela établit une correspondance entre le nom d'hôte et chacune de ses adresses IP d'interface. Pour atteindre l'hôte, utilisez la commande **telnet** ou **ping** avec le nom du routeur ou une adresse IP qui est associée au nom du routeur.

La procédure de configuration de la table d'hôtes est la suivante:

1. Passez en mode de configuration globale sur le routeur.
2. Entrez la commande **ip host**, suivie du nom du routeur et de toutes les adresses IP associées aux interfaces sur chaque routeur.
3. Continuez jusqu'à ce que tous les routeurs du réseau soient entrés.
4. Enregistrez la configuration en mémoire NVRAM.

m. Sauvegarde de la configuration

La configuration des équipements réseau détermine comment le réseau va se comporter. La gestion de la configuration des équipements comprend les tâches suivantes:

- Listage et comparaison les fichiers de configuration sur les équipements actifs
- Stockage des fichiers de configuration sur les serveurs de réseau
- Installations et mises à niveau de logiciels

Les fichiers de configuration doivent être stockés en tant que fichiers de sauvegarde pour parer à toute éventualité. Les fichiers de configuration peuvent être stockés sur un serveur réseau, sur un serveur TFTP ou encore sur un disque stocké en lieu sûr. La documentation doit être incluse avec ces informations hors connexion.

Une copie actuelle de la configuration peut être stockée sur un serveur TFTP. La commande **copy running-config tftp**, peut être utilisée pour stocker la configuration actuelle sur le serveur TFTP du réseau.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```

Pour ce faire, procédez comme suit :

Étape 1: Entrez la commande **copy running-config tftp**.
Étape 2: Entrez l'adresse IP de l'hôte où sera stocké le fichier de configuration.
Étape 3: Entrez le nom que vous voulez attribuer au fichier de configuration.
Étape 4: Confirmez vos choix en répondant oui à chaque fois.

Un fichier de configuration stocké sur l'un des serveurs du réseau peut être utilisé pour configurer un routeur. Pour ce faire, procédez comme suit:

1. Passez en mode configuration en entrant la commande **copy tftp running-config**,

```
router#copy tftp running-config

Host or network configuration file [host]?

IP address of remote host [255.255.255.255]? 131.108.2.155

Name of configuration file [Router-config]? tokyo.2

Configure using tokyo.2 from 131.108.2.155? [confirm] y

Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]

tokyo#
```

2. À l'invite du système, sélectionnez un fichier de configuration d'hôte ou de réseau. Le fichier de configuration de réseau comprend des commandes qui s'appliquent à tous les routeurs et serveurs de terminaux du réseau. Le fichier de configuration d'hôte comprend des commandes qui s'appliquent à un seul routeur. À l'invite du système, entrez l'adresse IP de l'hôte distant où se trouve le serveur TFTP. Dans cet exemple, le routeur est configuré à partir du serveur TFTP qui se trouve à l'adresse IP 131.108.2.155.

3. À l'invite du système, entrez le nom du fichier de configuration ou acceptez le nom par défaut. Le nom du fichier est basé sur les conventions d'appellation d'UNIX. Le nom de fichier par défaut est **hostname-config** pour le fichier hôte et **network-config** pour le fichier de configuration de réseau. Dans un environnement DOS, les noms de fichier sont limités à huit caractères, avec une extension de trois caractères (par exemple, **router.cfg**). Confirmez le nom du fichier de configuration et l'adresse du serveur TFTP fournis par le système. Dans la figure 2, notez que l'invite du routeur affiche immédiatement le nom **tokyo**. Vous avez ainsi la preuve que la reconfiguration est effective dès que le nouveau fichier est téléchargé.

La configuration du routeur peut être également sauvegardée en capturant le texte dans le routeur et en l'enregistrant sur une disquette ou sur un disque dur. Si vous devez recopier le fichier sur le routeur, utilisez les fonctions d'édition standard du programme émulateur de terminal pour coller le fichier de commandes dans le routeur.

C. Routage statique.

I. Présentation du routage statique

Étant donné que les routes statiques doivent être configurées manuellement, toute modification de la topologie réseau oblige l'administrateur à ajouter et supprimer des routes statiques pour tenir compte des modifications. Dans un grand réseau, cette maintenance manuelle des tables de routage peut générer une forte charge de travail administratif. Sur les petits réseaux où peu de modifications sont possibles, les routes statiques ne requièrent que très peu de maintenance. En raison des impératifs administratifs, le routage statique n'offre pas la même évolutivité que le routage dynamique. Même dans les grands réseaux, les routes statiques qui sont prévues pour atteindre un but précis sont souvent configurées en conjonction avec un protocole de routage dynamique.

II. Utilisation de la route statique

Les opérations de routage statique s'articulent en trois parties:

- L'administrateur réseau configure la route
- Le routeur insère la route dans la table de routage
- Les paquets sont acheminés à l'aide de la route statique

Puisqu'une route statique est configurée manuellement, l'administrateur doit la configurer sur le routeur à l'aide de la commande **ip route**. La syntaxe correcte de la commande **ip route** est illustrée à la figure suivante

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s0
```
commande

Dans les figures 2 et 3, l'administrateur réseau du routeur Hoboken doit configurer une route statique qui pointe sur les réseaux 172.16.1.0/24 et 172.16.5.0/24 liés aux autres routeurs. L'administrateur peut entrer l'une ou l'autre des deux commandes pour atteindre cet objectif. La méthode de la figure 2 spécifie l'interface sortante. La méthode de la figure 3 spécifie l'adresse IP du saut suivant du routeur adjacent. L'une ou l'autre des commandes insèrera une route statique dans la table de routage du routeur Hoboken.

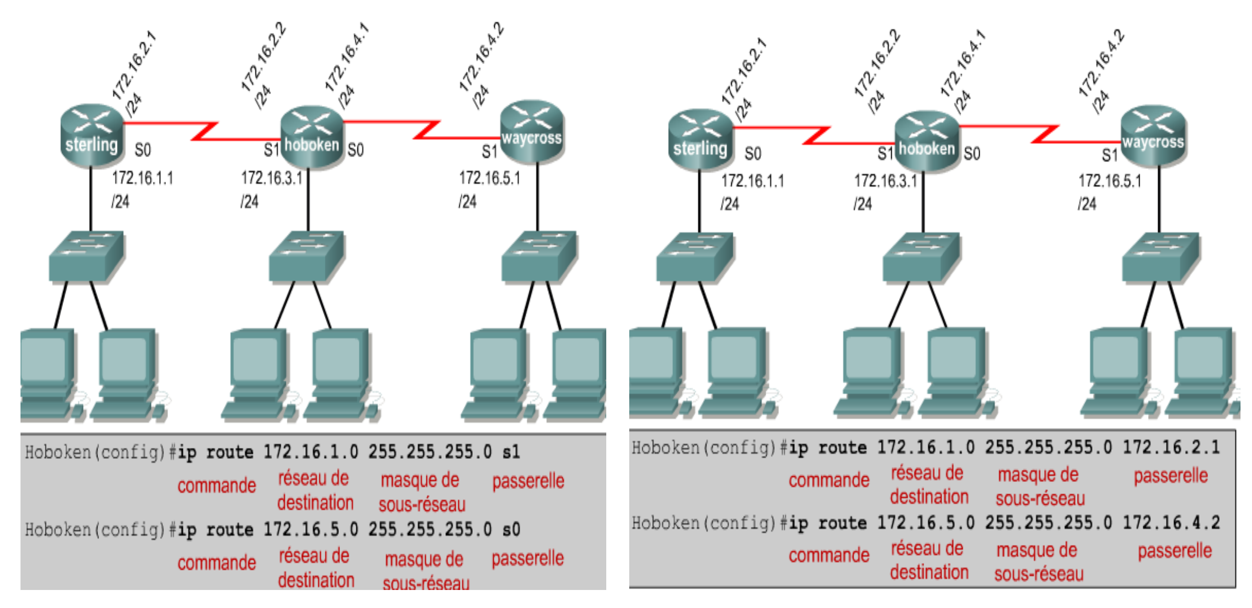


Figure 1 Figure 2

La distance administrative est un paramètre optionnel qui donne une mesure de la fiabilité de la route. Plus la valeur de la distance administrative est faible et plus la route est fiable. Ainsi, une route dont la distance administrative est faible sera insérée avant une route identique dont la distance administrative est élevée. La

distance administrative par défaut est 1 quand on utilise une route statique. Lorsqu'une interface de sortie est configurée comme passerelle dans une route statique, la route statique apparaît comme étant directement connectée. Ceci peut parfois porter à confusion, car une route vraiment directement connectée a une distance administrative de 0. Pour vérifier la distance administrative d'une route donnée. Utilisez la commande show ip route adresse, où l'option adresse est l'adresse IP de cette route. Si l'on souhaite une distance administrative autre que celle par défaut, il faut entrer une valeur comprise entre 0 et 255 après le saut suivant ou l'interface sortante:

waycross(config)#**ip route 172.16.3.0 255.255.255.0 172.16.4.1 130**

Si le routeur ne peut pas atteindre l'interface sortante qui est empruntée sur la route, la route n'est pas installée dans la table de routage. Cela veut dire que si cette interface est arrêtée, la route n'est pas inséré dans la table de routage.

Les routes statiques sont quelques fois utilisées à des fins de sauvegarde. Il est possible de configurer sur un routeur une route statique qui ne sera utilisée qu'en cas d'échec de la route acquise de façon dynamique. Pour utiliser une route statique de cette manière, attribuez simplement une valeur de distance administrative supérieure à celle du protocole de routage dynamique utilisé.

III. Configuration de routes statiques

Cette section décrit les étapes de configuration des routes statiques et donne un exemple de réseau simple pour lequel des routes statiques peuvent être configurées.

Pour configurer des routes statiques, procédez comme suit:

Étape 1: Déterminez tous les préfixes, masques et adresses désirés. Les adresses peuvent être soit une adresse locale, soit une adresse de saut suivant qui mène à l'adresse désirée.

Étape 2: Passez en mode de configuration globale.

Étape 3: Tapez la commande **ip route** avec une adresse de destination et un masque de sous-réseau, suivis de la passerelle correspondante de l'étape 1. L'inclusion d'une distance administrative est facultative.

Étape 4: Répétez l'étape 3 pour autant de réseaux de destination que définis à l'étape 1.

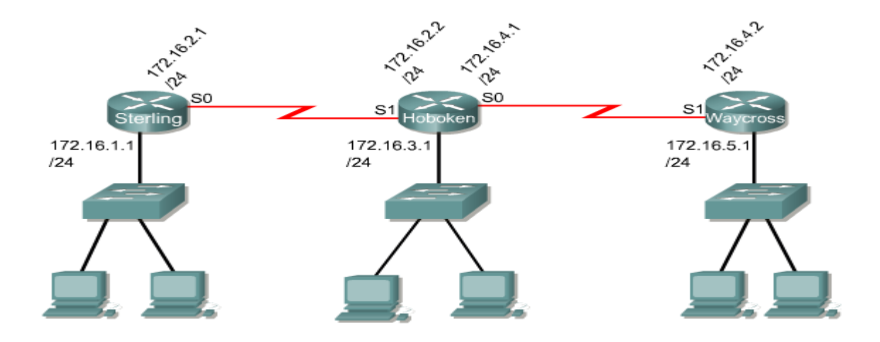
Étape 5: Quittez le mode de configuration globale.

Étape 6: Enregistrez la configuration courante en mémoire NVRAM en utilisant la commande **copy running-config startup-config**.

Le réseau de l'exemple est une configuration simple comportant trois routeurs. 1 Hoboken doit être configuré de façon à pouvoir atteindre le réseau 172.16.1.0 et le réseau 172.16.5.0. Ces deux réseaux possèdent un masque de sous-réseau 255.255.255.0.

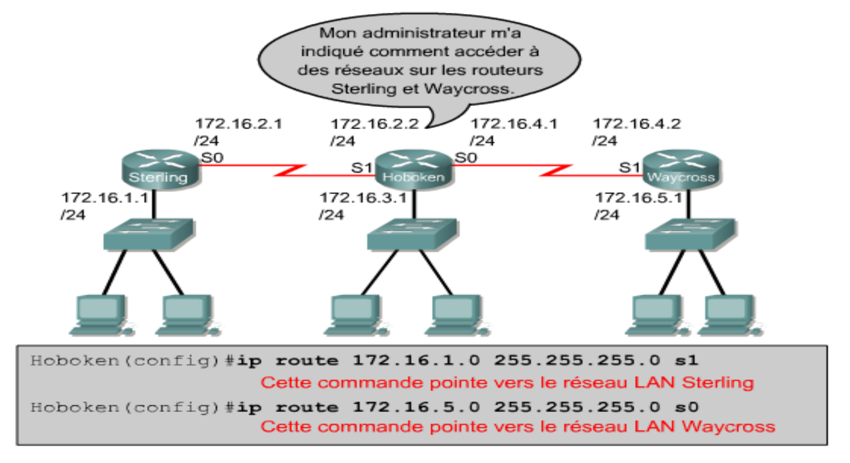
Les paquets dont le réseau de destination est 172.16.1.0 doivent être acheminés vers Sterling et ceux dont l'adresse de destination est 172.16.5.0 doivent être routés vers Waycross. Vous pouvez configurer des routes statiques pour accomplir cette tâche.

Les deux routes statiques seront d'abord configurées pour utiliser une interface locale comme passerelle vers les réseaux de destination.



Comme l'adresse administrative n'a pas été spécifiée, elle prendra la valeur 1 par défaut quand la route est installée dans la table de routage.

Les deux mêmes routes statiques peuvent également être configurées à l'aide d'une adresse du saut suivant comme passerelle.



La première route vers le réseau 172.16.1.0 possède une passerelle 172.16.2.1. La deuxième route vers le réseau 172.16.5.0 a une passerelle 172.16.4.2

Configuration de l'acheminement par défaut

Les routes par défaut permettent de router des paquets dont les destinations ne correspondent à aucune autre route de la table de routage. Les routeurs sont généralement configurés avec une route par défaut pour le trafic destiné à Internet, puisqu'il est souvent incommode et inutile de maintenir des routes vers tous les réseaux d'Internet. Une route par défaut est en fait une route statique spéciale qui utilise le format:

ip route 0.0.0.0 0.0.0.0 [*adresse de saut suivant* | *interface de sortie*]

Le masque 0.0.0.0, lorsque lié par un ET logique à l'adresse IP de destination du paquet à acheminer, générera toujours le réseau 0.0.0.0. Si le paquet ne correspond pas à une route plus spécifique de la table de routage, il sera acheminé vers le réseau 0.0.0.0.

Pour configurer des routes par défaut, procédez comme suit:

Étape 1 Passez en mode de configuration globale.

Étape 2 Entrez la commande **ip route** avec 0.0.0.0 comme préfixe et 0.0.0.0 comme masque. L'option adresse de la route par défaut peut être soit l'interface du routeur local qui permet de se connecter vers l'extérieur, soit l'adresse IP du routeur dans le saut suivant

Étape 3 Quittez le mode de configuration globale.

Étape 4 Enregistrez la configuration courante en mémoire NVRAM en utilisant la commande **copy running-config startup-config**.

Dans la section Configuration de routes statiques, les routes statiques ont été configurées sur le routeur Hoboken pour rendre accessibles les réseaux 172.16.1.0 sur Sterling et 172.16.5.0 sur Waycross. Il doit à présent être possible d'acheminer des paquets vers ces deux réseaux à partir d'Hoboken. Cependant, ni Sterling ni Waycross ne sauront comment retourner des paquets à un réseau non directement connecté. Une route statique pourrait être configurée sur Sterling et Waycross, pour chacun des réseaux de destination non directement connectés. Cela ne serait pas une solution assez évolutive dans le cas d'un grand réseau.

Le routeur Sterling se connecte à tous les réseaux non directement connectés via l'interface série 0. Le routeur Waycross a uniquement une connexion à tous les réseaux non directement connectés, via l'interface série 1. Une route par défaut sur Sterling et Waycross assurera le routage de tous les paquets qui sont destinés aux réseaux non directement connectés.

Vérification de la configuration de route statique

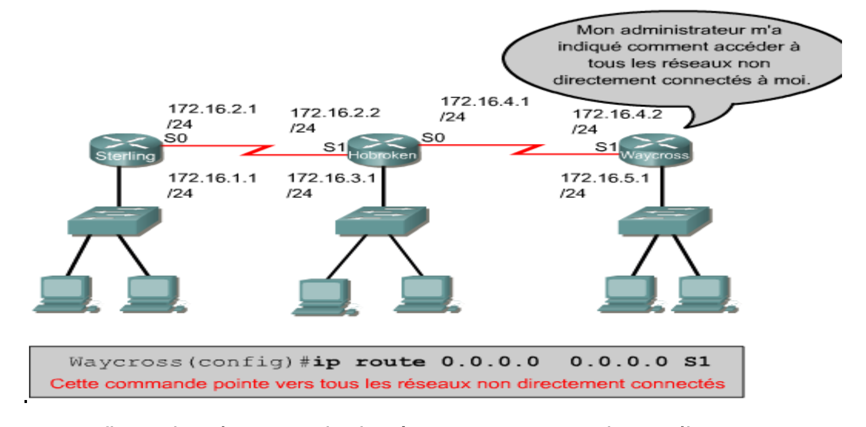
Une fois les routes statiques configurées, il est important de vérifier qu'elles figurent dans la table de routage et que le routage fonctionne comme prévu. La commande **show running-config** permet de visualiser la configuration courante en mémoire RAM afin de vérifier que la route statique a été entrée correctement. La commande **show ip route** permet quant à elle de s'assurer que la route statique figure bien dans la table de routage.

Pour vérifier la configuration des routes statiques, procédez comme suit:

- En mode privilégié, entrez la commande **show running-config** pour visualiser la configuration courante.
- Vérifiez que la route statique a été correctement entrée. Si la route n'est pas correcte, il vous faudra repasser en mode de configuration globale pour supprimer la route statique incorrecte et en insérer une correcte.
- Entrez la commande **show ip route**.
- Vérifiez que la route qui a été configurée figure dans la table de routage.

Dépannage de la configuration de route statique

Dans la section «Configuration des routes statiques», nous avons configuré des routes statiques sur le routeur Hoboken pour rendre accessibles les réseaux 172.16.1.0 sur Sterling et 172.16.5.0 sur Waycross



Si nous utilisons cette configuration, les noeuds du réseau 172.16.1.0 de Sterling ne peuvent atteindre ceux du réseau 172.16.5.0. À partir du mode privilégié sur le routeur Sterling, utilisez la commande ping vers un nœud du réseau 172.16.5.0. Cette commande échoue.

```
Hoboken#show ip route
Codes:C-connected,S-static,I-IGRP,R-RIP,M-mobile,B-BGP
D-EIGRP,EX-EIGRP external,O- OSPF,IA-OSPF inter area
N1-OSPF NSSA external type 1,N2-OSPF NSSA external type2
E1-OSPF external type 1,E2-OSPF external type 2, E - EGP
i-IS-IS,L1-IS-IS level-1,L2-IS-IS level-2,ia-IS-IS inter
area
* -candidate default, U - per-user static route, o - ODR
P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.4.0 is directly connected, Serial0
S       172.16.5.0 is directly connected, Serial0
S       172.16.1.0 is directly connected, Serial1
C       172.16.2.0 is directly connected, Serial1
```

Maintenant utilisez la commande traceroute de Sterling vers l'adresse qui a été utilisée précédemment avec la commande ping. Prenez note de l'endroit où la commande traceroute échoue. Elle indique que le paquet ICMP a été renvoyé depuis Hoboken mais pas depuis Waycross. Le problème se situe donc au niveau d'Hoboken ou de Waycross. Établissez une connexion Telnet avec le routeur Hoboken. Tentez à nouveau d'exécuter une

commande ping sur le noeud du réseau 172.16.5.0 connecté au routeur Waycross. Elle doit aboutir, car Hoboken est directement connecté à Waycross.

```
Sterling#ping 172.16.5.1
Type escape sequence to abort.
Sending 5,100-byte ICMP Echos to 172.16.5.1,timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

```
Sterling#traceroute 172.16.5.1
Type escape sequence to abort.
Tracing the route to 172.16.5.1
  1 172.16.2.2 16 msec 16 msec 16 msec
  2 172.16.4.2 32 msec 28 msec *
  3  *   *   *
  4  *   *   *
  5  *   *   *
  6  *   *   *
```

D. Présentation des protocoles de routage dynamique.

1. Introduction aux protocoles de routage

Les protocoles de routage différent des protocoles routés sur le plan de la fonction comme de la tâche.

Un protocole de routage est le système de communication utilisé entre les routeurs. Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur les réseaux à proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à construire et à mettre à jour une table de routage.

Exemples:

- Protocole d'informations de routage RIP (Routing Information Protocol)
- Protocole IGRP (Interior Gateway Routing Protocol)
- Protocole EIGRP (Enhanced Interior Gateway Routing Protocol)
- Protocole OSPF (Open Shortest Path First)

Un protocole routé sert à diriger le trafic utilisateur. Il fournit suffisamment d'informations dans son adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre.

Exemples :

- Le protocole Internet (IP)
- Le protocole IPX (Internetwork Packet Exchange)

2. Rôles d'un protocole de routage

- Le rôle d'un protocole de routage est de construire et mettre à jour la table de routage. Cette table contient les réseaux acquis et les ports associés à ces réseaux. Les routeurs utilisent des protocoles de routage pour gérer des informations reçues d'autres routeurs, les informations acquises de la configuration de ses propres interfaces, ainsi que des routes configurées manuellement.
- Le protocole de routage prend connaissance de toutes les routes disponibles. Il insère les meilleures routes dans la table de routage et supprime celles qui ne sont plus valides. Le routeur utilise les informations de la table de routage pour transmettre les paquets de protocole routé.
- L'algorithme de routage est une composante essentielle du routage dynamique. Chaque fois que la topologie du réseau est modifiée en raison de la croissance, d'une reconfiguration ou d'une panne, la base de connaissances du réseau doit également être modifiée.
- Lorsque tous les routeurs d'un interréseau reposent sur les mêmes connaissances, on dit de l'interréseau qu'il a convergé. Une convergence rapide est préférable, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces.

3. Systèmes autonomes

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune. Pour le monde extérieur, un système autonome est perçu comme une entité unique.

Les systèmes autonomes (AS) assurent la division de l'interréseau global en réseaux plus petits et plus faciles à gérer. Chaque système autonome possède son propre ensemble de règles et de politiques et un numéro AS unique qui le distinguera des autres systèmes autonomes à travers le monde.

L'InterNIC (*Internet Network Information Center*), un fournisseur de services ou encore un administrateur attribue un numéro d'identification à chaque système autonome. Ce numéro est un nombre à 16 bits. Les protocoles de routage, tels que l'IGRP de Cisco, nécessitent l'attribution d'un numéro de système autonome unique.

4. Identification des classes des protocoles de routage

La plupart des algorithmes de routage peuvent être rangés dans l'une des catégories suivantes:

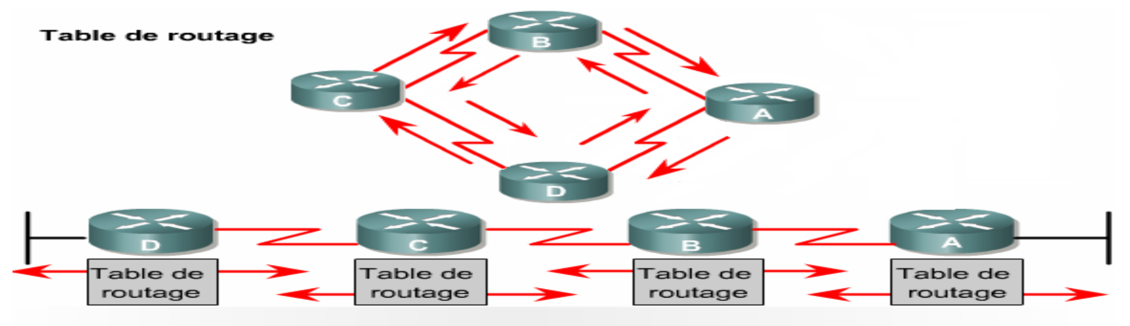
- vecteur de distance
- état de liens

Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'interréseau. L'approche à état de liens, également appelée routage par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau.

E. Protocoles de routage à vecteur de distance.

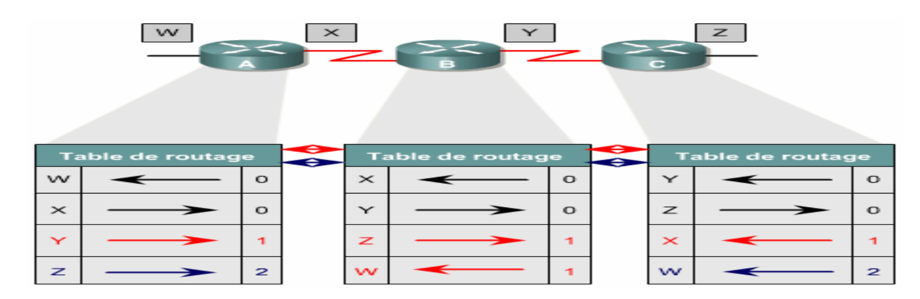
1. Fonctions du protocole de routage à vecteur de distance

Les algorithmes de routage à vecteur de distance transmettent régulièrement des copies de table de routage d'un routeur à l'autre. Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques. Chaque routeur reçoit une table de routage des routeurs voisins auxquels il est directement connecté.



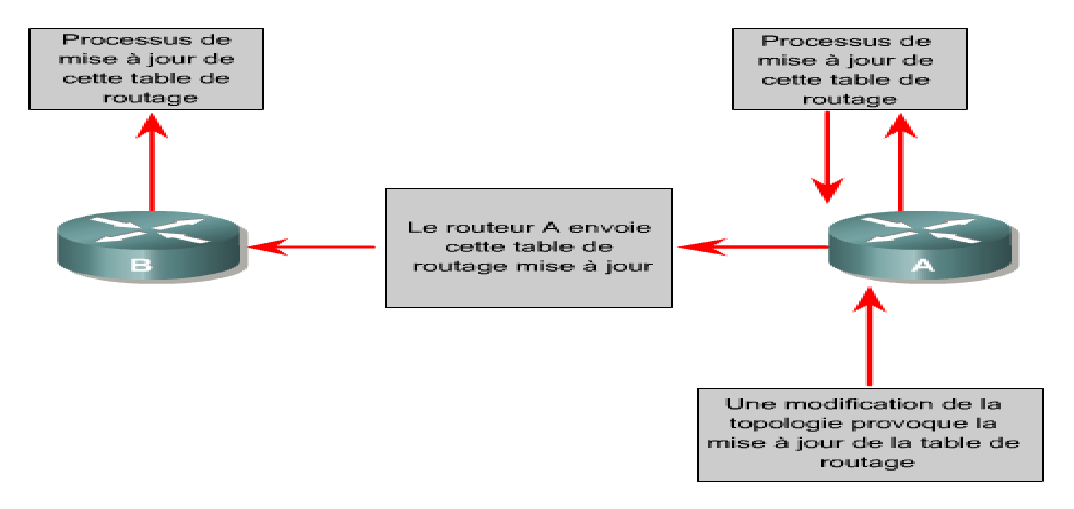
Le routeur B reçoit des informations du routeur A. Le routeur B ajoute un nombre de vecteurs (par exemple, un nombre de sauts) qui allonge le vecteur de distance. Ensuite, le routeur B transmet la nouvelle table de routage à son voisin, le routeur C. La même procédure est répétée étape par étape dans toutes les directions entre les routeurs directement adjacents.

Chaque routeur utilisant le routage à vecteur de distance commence par identifier ses voisins.



Les algorithmes à vecteur de distance prévoient que chaque routeur transmettra aux routeurs voisins l'intégralité de sa table de routage. L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau. Cependant, les algorithmes de routage à vecteur de distance ne permettent pas à un routeur de connaître la topologie exacte d'un interréseau, étant donné que chaque routeur voit uniquement ses voisins.

Lorsque la topologie change, les tables de routage sont mises à jour. Comme dans le cas du processus de découverte de réseau, la mise à jour des modifications topologiques s'effectue étape par étape, d'un routeur à l'autre.



F. Protocoles de routage RIP version 1 et version 2.

Le protocole RIP a été initialement défini dans la RFC 1058. Ses principales caractéristiques sont les suivantes:

- Il s'agit d'un protocole de routage à vecteur de distance.
- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

I. Algorithme général de RIP

Examinons un peu plus en détail le fonctionnement de RIP. Lors de l'initialisation du routeur, celui-ci détermine l'adresse réseau de ses interfaces puis envoie sur chacune une demande d'informations (table RIP complète) aux routeurs voisins. Lors de la réception d'une demande, un routeur envoie sa table complète ou partielle suivant la nature de cette demande. Lors de la réception d'une réponse, il met à jour sa table si besoin. Trois cas peuvent se présenter :

- pour une nouvelle route, il incrémente la distance, vérifie que celle-ci est strictement inférieure à 15 et diffuse immédiatement le vecteur de distance correspondant,
- pour une route existante mais avec une distance plus faible, la table est mise à jour. La nouvelle distance et, éventuellement, l'adresse du routeur si elle diffère sont intégrées à la table,
- pour une route existante mais avec une distance plus importante, la table est mise à jour si la nouvelle distance est émise par le même routeur voisin que précédemment.

Bien sûr, si l'appareil reçoit une route dont la distance est supérieure à celle déjà connue d'un autre voisin, RIP l'ignore. Ensuite, à intervalles réguliers (toutes les 30 secondes), la table RIP est diffusée qu'il y ait ou non des modifications.

Des routes doivent être retirées de la table gérée par RIP dans deux situations :

i. En premier lieu, si un réseau immédiatement connecté devient inaccessible (panne de l'interface, de la ligne, modification de la topologie par l'administrateur, etc.), les routeurs RIP reliés à ce réseau affectent dans leur table une distance «infinie» (16 comme indiqué plus haut) à cette route. Elle est conservée pendant la durée d'un temporisateur de «maintien» (*garbage collect*) de 120 secondes puis est supprimée. Immédiatement après, le vecteur avec une distance «infinie» est diffusé. Un routeur qui reçoit un vecteur avec une distance de 16 comprend : «il faut que tu retires cette route de ta table car elle est devenue invalide !» De proche en proche, cette information se propage.

ii. En second lieu, si un routeur du réseau tombe en panne. Cela veut peut-être dire que les réseaux situés derrière cet appareil sont devenus inaccessibles. Mais comment savoir si un routeur est en panne ? RIP considère qu'un routeur qui n'a pas donné de nouvelles depuis trois minutes est hors service. Pour gérer cette situation, il attribue à toutes les routes dynamiques un temporisateur initialisé à 180 secondes par défaut. A chaque réception d'un vecteur de distance déjà présent dans la table, le compteur est réinitialisé. Mais si jamais ce compteur atteint zéro, la route est considérée comme invalide. On se retrouve alors dans la situation précédente (distance infinie, temporisateur de maintien, diffusion de l'information puis suppression de la route). Maintenant, si un autre routeur connaît une route menant vers un des réseaux que l'on vient de retirer, c'est parfait ! Notre routeur intègrera cette nouvelle route dans sa table. De cette façon, RIP permet la tolérance aux pannes.

Comment justifier l'existence de ces mécanismes qui peuvent paraître un peu complexes ? Cela est dû à une faiblesse des algorithmes à vecteurs de distance que l'on appelle «problème de la convergence lente». Dans certains cas, après la panne d'un accès réseau, deux routeurs voisins risquent de se transmettre mutuellement puis, ensuite, de propager des informations contradictoires au sujet de ce réseau et créer ainsi une boucle de routage infinie. Les mécanismes suivants sont mis en place pour améliorer le RIP:

- ***split horizon* :** Une information de routage reçue sur une interface n'est jamais retransmise sur celle-ci.
- ***poison reverse* :** Les mises à jour de routage *poison reverse* appliquent une métrique «infinie» aux routes transmises par l'interface d'émission. Ce type de mise à jour aide à prévenir les boucles de routage.
- ***triggered update* :** Une panne est immédiatement diffusée sans attendre le prochain cycle de diffusion des tables afin de réduire le délai de convergence.

II. Améliorations de RIPv2 par rapport à RIPv1

Même si les principes évoqués ci-dessus sont valables quelle que soit la version de RIP, les différences restent intéressantes à relever. Les améliorations de RIPv2 sont :

- Diffusion des masques de sous-réseaux associés aux adresses réseaux (RIPv1 n'utilisait que les masques réseau par défaut).
- Utilisation d'une adresse de ***multicast*** pour diffuser les vecteurs de distance au lieu de l'adresse de ***broadcast*** ; ce qui réduit l'encombrement sur le réseau.
- Support de l'authentification en transportant un mot de passe crypté avec MD5.
- Interopérabilité entre protocoles de routage en diffusant des routes apprises à partir d'autres protocoles.

L'ensemble de ces raisons rend RIPv1 obsolète bien qu'il soit encore supporté par la plupart des routeurs logiciels ou matériels.

III. Configuration de RIPv1 et RIPv2

Voici un exemple de configuration de routage RIPv1:

GAD(config)#**router rip**
GAD(config-router)#**network 172.16.0.0**

Voici un exemple de configuration de routage RIPv2:

GAD(config)#**router rip**
GAD(config-router)#**version 2**
GAD(config-router)#**network 120.0.0.0**
GAD(config-router)#**network 172.16.0.0**
GAD(config-router)#**network 194.200.130.0**

Les numéros de réseau sont basés sur les adresses de classe, et non sur les adresses de sous-réseau ou des adresses hôtes. Les principales adresses réseau se limitent aux numéros de réseau des classes A, B et C.

G. Table de routage : examen détaillé.

1. Commande show ip route

- Show ip route → affiche le contenu de la table de routage IP.
- Show ip route connected → affiche les routes directement connectés « C »
- Show ip route {address} → affiche les entrée routant vers une destination particulier.
- Show ip route rip → affiche les routes RIP « R »
- Show ip route igrp → affiche les routes IGRP « I »
- Show ip route static → affiche les routes manuellement configurés.

2. Détermination de la passerelle de dernier recours

Les routes par défaut sont utilisées lorsque le routeur est incapable d'associer un réseau de destination à une entrée spécifique de la table de routage.

Avantage : les tables de routage ne sont pas encombrées.

La commande show ip route affiche ce qui suit :

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

3. Détermination de la dernière mise à jour de routage

Show ip route

```
Gateway of last resort is not set

R  200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14,
Serial0/0
C  192.168.10.0/24 is directly connected, Serial0/0
C  192.168.0.0/24 is directly connected, Loopback0
```

Show ip protocols

```
rt1#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 9
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 1, receive
any version
   Interface        Send Recv Triggered RIP Key-chain
   Serial0/0        1    1 2
   Loopback0        1    1 2
 Routing for Networks:
   192.168.0.0
   192.168.10.0
```

Show ip rip database

```
rt1#show ip rip database
192.168.0.0/24   auto-summary
192.168.0.0/24   directly connected, Loopback0
192.168.10.0/24   auto-summary
192.168.10.0/24   directly connected, Serial0/0
200.200.200.0/24   auto-summary
200.200.200.0/24
[1] via 192.168.10.2, 00:00:20, Serial0/0
```

H. Protocole EIGRP.

1. Qu'est-ce que IGRP ?

IGRP *(*Interior Gateway Routing Protocol), développé par Cisco, peut être considéré comme un protocole de routage à vecteur de distance. Il possède quelques caractéristiques qui le distinguent des autres protocoles à vecteur de distance tels que RIP. Parmi ces caractéristiques, notons son insensibilité à la taille du réseau, une réponse rapide aux modifications de réseaux, une métrique sophistiquée et la gestion des chemins multiples.
N.B. IGRP ne supporte pas les masques de sous-réseaux de taille variable.

a. Comment configurer IGRP ?
Pour configurer IGRP, utilisez les commandes suivantes :
Router igrp système autonome
Network numéro_réseau
Par exemple
ROUTER IGRP *150* active le processus *IGRP* pour le système autonome *150.*
NETWORK *10.0.0.0* associe le réseau 10.0.0.0 au routage *IGRP.*

b. Comment déterminer les réseaux découverts par le protocole IGRP ?
Les réseaux découverts par le protocole IGRP sont précédés de la lettre I. Les réseaux connectés directement au routeur et configurés via la commande NETWORK sont précédés de la lettre C.
Pour afficher la table de routage, il faut utiliser la *commande* suivante :
SHOW IP ROUTE. Les routes IGRP sont *indiqués* par un I.

2. Qu'est-ce que EIGRP (Enhanced IGRP) ?

EIGRP *(Enhanced* Interior Gateway Routing Protocol), développé par Cisco, est une version avancée de IGRP. Bien que basé sur un algorithme de routage à vecteur de distance identique à celui d'IGRP, ce protocole dispose d'une meilleure convergence grâce à l'utilisation de l'algorithme DUAL.
EIGRP (IGRP Avancé) est un protocole propriétaire qui combine les avantages des protocoles de routage à état de liaison et des protocoles à vecteur de distance. C'est un protocole hybride.
Il utilise les messages HELLO, mais l'échange des mises à jour des routes est basé sur le mécanisme vecteur de distance.
Pour la sélection des routes, l'algorithme employé est totalement différent des protocoles à vecteur de distance ou à état de liaison.
EIGRP utilise une métrique composée de la bande passante, du délai, de la charge et de la fiabilité afin de calculer le meilleur chemin entre deux correspondants.
EIGRP est capable de router IP, IPX et AppleTalk.
Le cœur de EIGRP est l'algorithme DUAL (Diffusing Update Algorlthm) qui garde une route de secours au cas où la route primaire est défaillante.
Avec EIGRP, il n'y a pas de limite avec le nombre de sauts.
Dans un réseau EIGRP, chaque routeur multicast envoie un message HELLO pour découvrir ses voisins immédiats. La table obtenue est partagée avec d'autres routeurs pour construire la topologie du réseau. A partir de la topologie du réseau, le routeur enregistre la meilleure route et la ou les routes de secours.
EIGRP est "classless", c'est-à-dire qu'il prend en compte les masques de sous-réseaux dans la mise à jour du routage.

3. Quelles sont les caractéristiques de EIGRP ?

Caractéristiques	RIP v1	RIP v2	OSPF	IGRP	EIGRP
Classfull or classless	**classfull**	**classless**	**classless**	**classsfull**	**classless**
Métrique	**nombre de sauts**	**nombre de sauts**	**coût (100.000.000/bw)**	**composé (BDRLM)**	**composé (BDRLM)**
Actualisation périodique	**30 secondes**	**30 secondes**	**non**	**90 secondes**	**30 secondes**
Adresse pour les annonces	**255.255.255.255 (broadcast)**	**224.0.0.9 (mutticast)**	**224.0.0.5 224.0.0.6 (multicast)**	**255.255.255.255 (broadcast)**	**224.0.0.10 (multicast)**
Distance administrative	**120**	**120**	**110**	**100**	**interne 90 externe 170**
catégorie	**vecteur de distance**	**vecteur de distance**	**à état de lien**	**Vecteur de distance**	**hybride**

4. Quels sont les avantages de EIGRP ?

- **Convergence rapide** : grâce à l'utilisation de l'algorithme DUAL (Diffusing Update Algorithm), chaque rouleur configuré pour utiliser EIGRP conserve des routes de secours pour s'adapter rapidement en cas de problèmes sur la route primaire. Si aucune alternative n'existe, EIGRP interroge ses voisins pour en découvrir une.
- **Réduction de l'utilisation de la bande passante** : conséquence du fait que EIGRP ne réalise pas d'actualisations périodiques. Des actualisations sont effectuées lorsque le chemin ou la métrique change pour cette route. L'algorithme DUAL envoie une actualisation ne concernant que le lien modifié (plutôt que toute la table) et uniquement vers les rouleurs qui en ont besoin.
- **Support de plusieurs couches réseau** : EIGRP supporte TCP/IP/ IPX/SPX, *APPLETALK*.
- **Vecteur de distance** : EIGRP n'est pas limité comme RIP à 16 sauts.

5. Comment fonctionne l'algorithme DUAL ?

L'algorithme DUAL *(Diffusing* Update Algorithm) est en partie responsable de la rapidité de convergence de EIGRP.
En utilisant DUAL, le protocole de routage maintient deux tables :

- Une table des voisins : les routeurs mettent à jour leurs tables des voisins à partir des informations transportées par les paquets HELLO.
- Une table de topologie : représente tous les réseaux qui existent dans le système autonome. Elle est construite à partir des paquets d'actualisation envoyés par les voisins.

Le but de DUAL est d'offrir une possibilité de choisir immédiatement un chemin alternatif sans boucle vers toute destination, lorsque le chemin primaire est en panne.

EIGRP n'a pas besoin d'informer les autres routeurs si le chemin alternatif est garanti sans boucle et ne modifie pas la distance calculée pour atteindre la destination.

EIGRP recalcule une nouvelle route suite à un des événements suivants :

- La réception d'un message d'actualisation qui modifie la distance vers le réseau de destination.
- Un routeur voisin est déclaré en panne car son message hello n'arrive pas.
- Une modification dans la distance du lien local.
- La réception d'un message d'interrogation ou de réponse.

EIGRP effectue d'abord un calcul local. Chaque chemin possible, vers la destination, est évalué. Si une route alternative répond au critère de vraisemblance (c'est-à-dire sans boucle de routage), EIGRP peut l'utiliser immédiatement pour transmettre le trafic.

6. Qu'est-ce qu'une distance EIGRP ?

Le protocole utilise la métrique pour comparer des chemins vers une destination et choisir le meilleur d'entre eux. Le protocole EIGRP emploie une métrique composite (BDRLM : Bandwidth Delay Reliability Load Metric) pour représenter la topologie inter-réseau et pour décider du routage d'un paquet.

Métrique = [K1 * bande passante + (K2 * bande passante)/(256-charge) + K3*délai] * [K5/(fiabilité + K4)]

Les valeurs par défaut des constantes sont K1 = K3 = 1 et K2 = K4 = K5 = 0.
Métrique = bande passante + délai

La métrique composite (BDRLM) ou distance EIGRP est la somme pondérée de cinq facteurs :

- Bande passante (Bandwidth) : le calcul de la métrique EIGRP dépend de façon importante du paramètre Bande passante, donc il faut choisir une bande passante correcte. Les interfaces LAN connaissent automatiquement leur bande passante alors que les interfaces série posent des problèmes. Pour choisir une métrique correcte sur des interfaces série, utilisez la commande BANDWITH.
  Par exemple :
  ```
  Router#Configure terminal
  Router#interface S0
  Router#bandwith 64000
  Router#end
  ```
- Retard (Delay) : le retard associe chaque type d'interface du routeur à une valeur de retard typique et additionne tous les retards du chemin du routeur source jusqu'au routeur de destination. Le tableau ci-après donne des exemples de valeurs de retard implicites par type d'interface. Notez aussi que toutes les interfaces série ont la même valeur retard.

Interface	Bande passante	Retard
Ethernet	10 Mbit/s	25 600 us
Série T1	1,544 Mbit/s	512 000 us

- Fiabilité (Reliability) : la composante fiabilité est un compteur sur 8 bits. Il est interprété comme le numérateur d'une fraction dont le dénominateur est toujours 255. Ainsi, une interface fiable est représentée par une composante de fiabilité valant 255.
- Charge (Load) : elle est représentée comme le numérateur d'une fraction dont le dénominateur est 255. Un routeur saturé a une composante de charge de 255, alors qu'un routeur peu chargé peut avoir une composante de charge de 1.

Par défaut, seulement deux des quatre composantes de la distance EIGRP sont utilisées dans le calcul de la métrique. Sauf modification volontaire, les facteurs de charge et de fiabilité ne sont pas pris en compte dans la métrique EIGRP. Les composantes Fiabilité et Charge sont exclues par l'introduction d'un facteur multiplicatif dans la formule de la distance.

7. Qu'est-ce que la distance administrative ?

La distance administrative est la mesure utilisée par les routeurs Cisco pour sélectionner le meilleur chemin quand il ya deux ou plusieurs routes différentes pour la même destination à partir de deux protocoles de routage différents. Cette distance définit la fiabilité ou la crédibilité d'un protocole de routage, par exemple un itinéraire IGRP sera choisi sur un itinéraire RIP version 2.

8. Quelles sont les commandes pour configurer un processus de routage EIGRP ?

La commande pour configurer EIGRP est :

Router EIGRP <système_autonome>

Pour spécifier un ensemble de réseaux au processus EIGRP :

Network <numéro_réseau>

Le numéro du réseau est l'identifiant d'une classe d'adressage d'un réseau connecté directement au routeur, ce qui comprend les sous-réseaux spécifiques configurés sur les interfaces correspondantes.

I. Protocoles de routage d'état des liaisons.

1. Fonctions du protocole de routage à état de liens

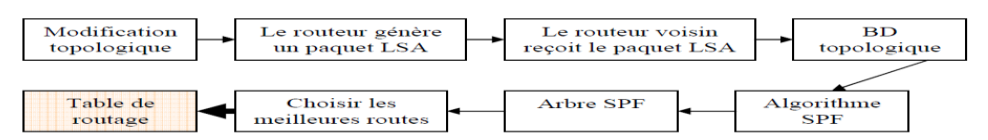
Le deuxième algorithme de base utilisé pour le routage est l'algorithme à état de liens.

- Ces algorithmes sont également appelés algorithme de Dijkstra ou algorithme SPF (shortest path first ou du plus court chemin d'abord).
- Ils gèrent une base de données complexe d'informations topologiques. L'algorithme à vecteur de distance comprend des informations non spécifiques sur les réseaux distants et ne fournit aucune information sur les routeurs distants.
- Un algorithme de routage à état de liens gère une base de connaissances complète sur les routeurs distants et leurs interconnexions.

Le routage à état de liens utilise les éléments suivants:

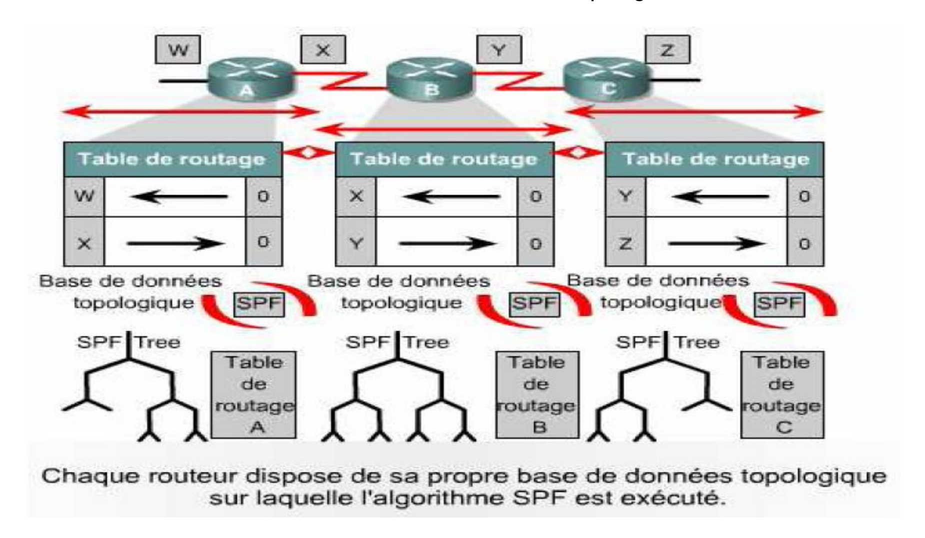
- Mises à jour de routage à état de liens (LSA : link-state advertisement) – Des petits paquets d'informations de routage qui sont transmis entre les routeurs.
- Base de données topologique – Une base de données topologique est un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liens.
- Algorithme SPF – L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.
- Tables de routage – Une liste des chemins et des interfaces connus.

2. Processus de découverte du réseau pour le routage à état de liens



Les mises à jour de routage à état de liens sont échangées entre routeurs en commençant par les réseaux directement connectés. Parallèlement à ses homologues, chaque routeur génère une base de données topologique comprenant toutes les mises à jour de routage à état de liens échangées.

L'algorithme du plus court chemin d'abord (SPF) calcule l'accessibilité aux réseaux. Le routeur génère cette topologie logique sous la forme d'un arbre dont il est la racine et qui comporte tous les chemins possibles menant à chaque réseau de l'interréseau utilisant le protocole à état de liens. Ensuite, il trie ces chemins sur la base du chemin le plus court. Le routeur répertorie dans sa table de routage les meilleurs chemins et les interfaces menant aux réseaux de destination. Il met également à jour d'autres bases de données contenant des éléments de topologie et les détails relatifs à leur état.



Chaque routeur dispose de sa propre base de données topologique sur laquelle l'algorithme SPF est exécuté.

3. Considérations relatives au routage à état de liens:

- Surcharge du système (Processeurs)
- Mémoire requise.
- Consommation de bande passante.

J. PROTOCOLE DE ROUTAGE OSPF.

1. Introduction

Le protocole OSPF (Open Shortest Path First) a été développé suite au besoin de la communauté Internet d'utiliser un protocole intérieur IGP (Internal Gateway Protocol) dans la pile des protocoles TCP/IP, non-propriétaire et hautement fonctionnel. Les discussions sur la création d'un IGP commun et inter-opérable pour l'Internet commença en 1988 et ne fut pas formalisé avant 1991.

OSPF est un protocole de couche 3, annoncé dans un paquet IP avec le numéro de protocole 89. Il n'utilise pas TCP pour la fiabilité qu'il assure par des mécanismes propres.

2. Comparatif fonctionnel des protocoles RIP et OSPF

La croissance rapide et l'expansion des réseaux ont poussé RIP à ses limites. RIP comporte certaines restrictions qui peuvent causer des problèmes dans les réseaux larges :

- **RIP a une limite de 15 sauts**. Un réseau qui comporte plus de 15 sauts (15 routeurs) est considéré comme inaccessible.
- **RIP ne supporte pas les masques à longueur variable (VLSM : Variable Length Subnet Mask)**. Compte tenu du manque d'adresses IP et de sa flexibilité, le VLSM comporte des avantages considérables dans les plans d'adressage.
- **L'envoi périodique de l'entièreté des tables de routage en diffusion *(broadcast)* consomme une grande quantité de bande passante**. Il s'agit d'un véritable problème dans les réseaux larges et spécifiquement sur les liaisons lentes et les nuages WAN.
- **RIP converge plus lentement qu'OSPF**. Dans les très grands réseaux, la convergence doit être rapide.
- **RIP ne prend pas en compte les paramètres de délai et de coût**. Les décisions de routage sont uniquement basées sur le nombre de sauts quelque soit la bande passante ou les délais des lignes.
- **Les réseaux RIP sont des réseaux plats**. Il n'y a pas de concept d'*area* (zone) ou de *boundarie* (frontière). Avec l'introduction du routage *classless* et l'utilisation intelligente de l'agrégation et de la *summurization* des routes, les réseaux RIP ont moins de succès.

Certaines améliorations ont été introduites dans une version nouvelle de RIP appelée RIP2. RIP2 supporte le VLSM, permet l'authentification et les mises à jour de routage multicast. Toutefois, ces améliorations restent faibles car RIP2 est encore limité par le nombre de sauts et une convergence lente qui conviennent mal aux réseaux étendus.

Voici les caractéristiques comparatives d'OSPF :

- **Il n'y a pas de limite du nombre de sauts**. OSPF étant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d'une zone (*area*). Aussi, le danger de boucles de routage n'étant *a priori* plus présent, la limite du nombre de sauts n'est plus nécessaire.
- **L'utilisation intelligente du VLSM améliore les plans d'adressage** (allocations d'adresses IP). Il supporte aussi l'agrégation et la summarization de routes.
- **Il utilise IP multicast pour envoyer ses mises à jour d'état de lien**. Cette méthode prend moins de ressources aux routeurs qui n'écoutent pas de paquets OSPF. Aussi, ces mises à jour sont envoyées uniquement lors d'un changement de topologie. On économise de manière évidente la bande passante. Les mises à jour sont seulement incrémentielles.
- **OSPF a une meilleure convergence que RIP** parce que les changements de routage sont propagés instantanément et non périodiquement de manière incrémentielle grâce aux relations de voisinage entretenues.
- **OSPF permet de segmenter le réseau en zones** pour limiter le trafic généré par les updates de routage à l'intérieur des zones.
- **OSPF est meilleur pour la répartition de charge** *(load balancing*).
- **Le choix du meilleur chemin est basé sur le coût (la bande passante inversée).** Cette métrique peut être définie manuellement sur les interfaces.
- **OSPF permet une définition logique des réseaux** où les routeurs peuvent être répartis en zones (*area).* Cela évitera une explosion de mises à jour d'états de lien sur l'ensemble du réseau. On peut également ainsi fournir un mécanisme d'agrégation des routes et stopper la propagation inutile des informations de sous-réseaux existants.
- **Il permet l'authentification de routage** par l'utilisation de différentes méthodes d'identification avec mots de passe.
- **Il permet le transfert et l'étiquetage des routes extérieures injectées dans un Système Autonome (AS)** pour permettre de les maintenir par des EGPs comme BGP.

3. Les éléments clés d'OSPF.

Les routeurs OSPF entretiennent une relation orientée connexion avec les routeurs d'un même segment physique. Dans la terminologie OSPF, on parlera d'*adjacency*, en français, d'adjacence ou de contiguïté.
Au lieu d'envoyer des mises à jour entières lors d'un changement topologique, OSPF envoie des mises à jour incrémentielles.

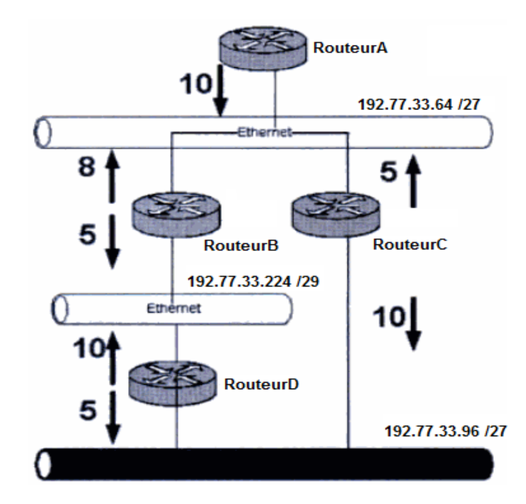
- OSPF n'est pas limité par une segmentation dépendante de l'adressage IP ou des sous-réseaux, il utilise la notion d'*area* pour désigner un groupe de routeurs.

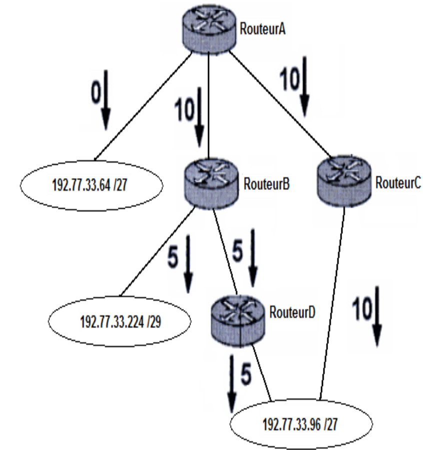
- OSPF supporte entièrement les possibilités du VLSM et de la *summarization* manuelle des routes.
- Grâce à la possibilité de donner des rôles particuliers aux routeurs, la communication inter-routeurs est efficace.
- Bien qu'OSPF permette une communication *inter-area*, il reste un protocole de routage intérieur (IGP).
- OSPF est un protocole à état de lien. L'état d'un lien est une description d'une interface du routeur et de la relation qu'elle entretient avec les routeurs voisins.
- Le coût ou la métrique d'une interface dans un réseau OSPF est inversement proportionnelle à la bande passante de l'interface. La formule utilisée pour calculer le coût est : (100 000 000/Bande passante)

  Par exemple :
  - Traverser une ligne à 10 Mbps coûtera 10
  - Traverser une ligne cadensée à T1(1,544 Mbit/s) coûtera 64

4. Qu'est-ce que le chemin le plus court ?

Sur le schéma ci-après toutes les interfaces ont un coût associé. Prenons le Routeur A comme racine de l'arbre et calculons tous les chemins les plus courts à partir de ce routeur.





Arbre des chemins OSPF possibles à partir du Routeur A

Dans cet exemple :

- Le Routeur A peut atteindre le réseau 192.77.33.224/29 via le Routeur B avec un coût de 15 (10+5)
- Le Routeur A peut aussi atteindre le réseau 192.77.33.96/27 via le Routeur C avec un coût de 20 (10+10) ou via le Routeur B avec un coût de 20 (10+5+5)

Nous avons donc deux chemins pour atteindre le réseau 192.77.33.96/27 avec le même coût. L'implémentation d'OSPF sur un routeur CISCO prend en compte le nombre de saut pour résoudre ce genre de conflits.

5. Hiérarchie

Une caractéristique principale d'OSPF est de supporter des inter-réseaux très larges. Elle est possible grâce au regroupement des routeurs dans des entités logiques appelées area ou zone.

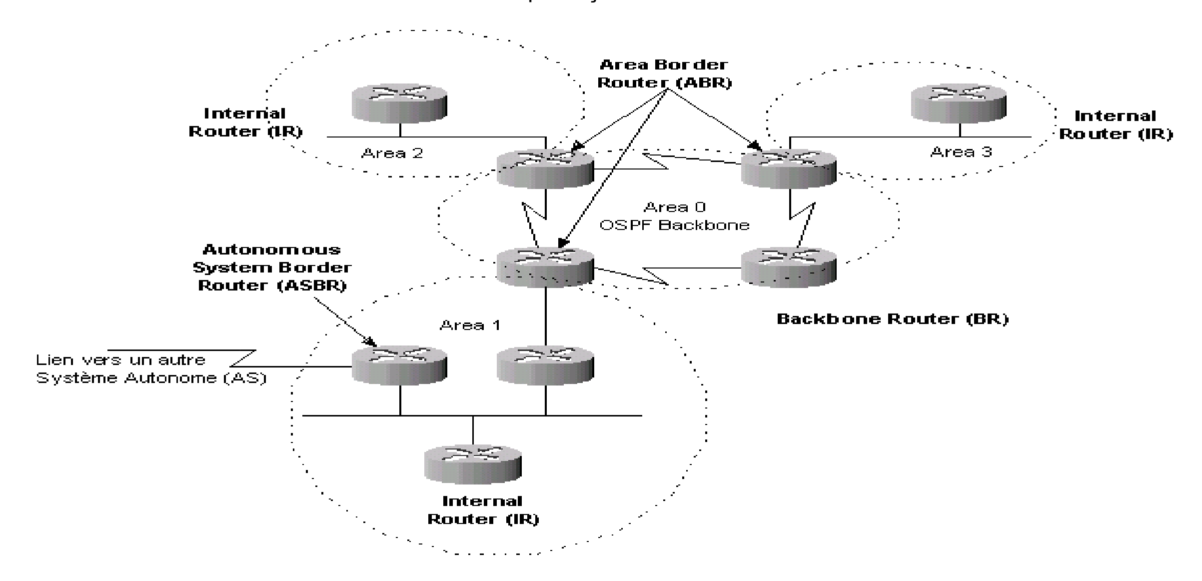
La communication inter-zones ne laisse passer l'échange d'informations minimales de routage uniquement pour que les zones restent connectées. Il en résulte que tous les efforts de calcul de routes ne s'opèrent qu'au sein d'une même zone. Les routeurs d'une zone ne sont pas affectés par les changements intervenus dans une autre zone. Dans un contexte où OSPF demande beaucoup de ressources en CPU et en mémoire, cette notion de conception est très importante.

Un routeur OSPF peut prendre en charge trois types d'opérations : opération dans une zone, connexion inter-zone et connexion entre systèmes autonomes (AS). Comme vu plus haut, pour remplir ces tâches, un routeur doit remplir un rôle et une responsabilité particulière qui dépend de l'hiérarchie OSPF établie.

- ***Internal Router* (IR)** : Un IR remplit des fonctions au sein d'une zone uniquement. Sa fonction primordiale est d'entretenir à jour sa base de donnée avec tous les réseaux de sa zone, sa base de donnée d'états de lien *(link-state database*), qui est identique sur chaque IR. Il renvoie toute information aux autres routeurs de sa zone, le routage ou l'inondation (*flooding*) des autres zones requiert l'intervention d'un *Area Border Router* (ABR).
- ***Backbone Router* (BR)** : Une des règles de conception OSPF est que chaque zone dans l'inter-réseau doit être connectée à une seule zone, la zone 0 ou la *backbone area*. La plupart des BR ont une interface connectée à la *backbone area* et une ou plusieurs interfaces à d'autres zones.
- ***Area Border Router* (ABR)** : Un ABR connecte deux ou plusieurs zones. Un ABR possède autant de bases de données d'états de lien qu'il y a d'interfaces connectées à des zones différentes. Chacune des ces bases de données contiennent la topologie entière de la zone connectée et peut donc être *summarizée,* c'est-à-dire agrégée

en une seule route IP. Ces informations peuvent être transmises à la zone de *backbone* pour la distribution. Un élément clé est qu'un ABR est l'endroit où l'agrégation doit être configurée pour réduire la taille des mises à jour de routage qui doivent être envoyées ailleurs. Donc quand on parle des capacités d'OSPF de minimiser les mises à jour de routage, on peut directement penser au rôle rempli par les ABR.

- ***Autonomous System Boundary Router* (ASBR) :** Il faut bien retenir qu'OSPF est un IGP (*Interior Gateway Protocol*), autrement dit qu'il devra être connecté au reste de l'Internet par d'autres AS. Ce type de routeur fera en quelque sorte office de passerelle vers un ou plusieurs AS. L'échange d'information entre un AS OSPF et d'autres AS est le rôle d'un ASBR et les informations qu'il reçoit de l'extérieur seront redistribuées au sein de l'AS OSPF.



6. Le fonctionnement d'OSPF dans une zone

Cette section traite du fonctionnement d'OSPF au sein d'une seule zone et de la manière dont la topology table ou la link-state database est construite. La table de routage est constituée à partir de cette base de données. Ce résultat est obtenu grâce à l'application de l'algorithme de routage SPF. En voici les différentes étapes.

1. D'abord, un routeur doit trouver ses voisins. Pour ce faire, il utilise des paquets Hello. Dès son initialisation ou à la suite d'un changement de routage, un routeur va générer un *link-state advertisement* (LSA). Cette annonce va représenter la collection de tous les états de liens de voisinage du routeur.
2. Tous les routeurs vont s'échanger ces états de liens par inondation (*flooding*). Chaque routeur qui reçoit des mises à jour d'état de lien (*link-state update*) en gardera une copie dans sa *link-state database* et propagera la mise à jour auprès des autres routeurs.
3. Après que la base de données de chaque routeur soit complétée, le routeur va calculer l'arbre du chemin le plus court (*Shortest Path Tree*) vers toutes les destinations avec l'algorithme Dijkstra. Il construira alors la table de routage (*routing table*), appelée aussi *forwarding database,* en choisissant les meilleures routes.
4. S'I n'y a pas de modification topologique, OSPF sera très discret. Par contre en cas de changement, il y aura échange d'informations par des paquets d'état de lien et l'algorithme Dijkstra recalculera les chemins les plus courts.

7. Comment activer OSPF sur un routeur ?

L'activation d'OSPF sur un routeur se fait avec les commandes suivantes :

router OSPF <identificateur du processus>
network <réseau ou adresse IP> <masque inversé> ***area*** <identificateur de la zone>

- <identificateur du processus> est une valeur numérique local à un routeur, nous pouvons faire tourner plusieurs processus OSPF sur le même routeur mais ceci n'est pas recommandé à cause de la charge CPU.
- <identificateur de la zone> est une valeur entière comprise entre 0 et 4294967295 ou une adresse IP A.B.C.D

Exemple :

Router OSPF 100
Network 192.77.33.64 0.0.0.31 area 0.0.0.0
Network 192.77.33.224 0.0.0.7 area 23

8. Comment afficher les informations sur un processus OSPF ?

Les commandes utilisées sont :

show IP OSPF
show IP OSPF BORDER-ROUTERS